Adaptive Security Slice Monitoring

João W. Cangussu
University of Texas at Dallas
Department of Computer Science
cangussu@utdallas.edu

Ram Dantu
University of North Texas
Department of Computer Science
rdantu@unt.edu

Workshop on GENI and Security

GLOBAL ENVIRONMENT FOR NETWORK INNOVATIONS

The Erik Jonsson School of Engineering and Computer Science

Motivation

- GENI will be hosting the testing of innovative networking techniques which can bring with them a series of new flaws that could be malicious or accidentally exploited.
- Security attacks can happen intentionally when running an experiment or it can be the consequence of a series of unexpected events.
- GENI should be prepare to identify the existing attacks and it should be able to learn how to identify any new attack. It should also be able to point out the causes of the attacks.

Proposed Solution

- Here we propose the use of Bayesian Belief Networks (BBNs) to model the cause-effect relationship between elements of a network experiment and associated attacks/flaws.
- Data is collected as experiments are running and used to create the structure of a BBN as well as to train it. In this way whenever an attack is identified the events leading to the attack are accounted for.
- The created BBN can be later used not only to identify the attack when other experiments are running but also to allow the computation of the probability of the attack under the occurrence of a series of events; it can sound an alarm when an attack or specific flaw is about to happen.
- The BBNs can be dynamically adapted/updated for any number of attacks and flaws, including newly discovered problems.

BBN Approach

- Observations extracted from system are stored in the source nodes (system configuration based on parameters values)
- Hypotheses regarding the state of the system are stored at the terminal nodes (security state of the system)
- We can run queries to determine the probability of a given attack as well as the source of the attack.
- The BBN is automatically constructed using algorithms to create the structure of the network based on collected data.
- Training the BBN is also based on data.
- New attacks can be dynamically incorporated to the BBN.

BBN Approach

Pi: Slice Monitored Parameters
Ai: Attacks/Security Issues

Experiments data is used to create the structure and the CPT of the BBN.